

## СОЦИАЛЬНАЯ СЕТЬ КАК АКТУАЛЬНЫЙ ИНСТРУМЕНТ ПРИ ВЫЯВЛЕНИИ, РАСКРЫТИИ И РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ

Надежда Анатольевна Моругина

*Воронежский институт МВД России, г. Воронеж, Россия*  
moruginy@mail.ru

**Аннотация.** В статье обосновываются перспективные направления использования информации, полученной из социальной сети (цифровой след) в целях выявления, раскрытия и расследования преступлений, приводится опыт Канады и России. Автор утверждает, что информация, содержащаяся на персональных страницах социальных сетей, позволяет идентифицировать личность подозреваемого/обвиняемого/свидетеля/потерпевшего, найти соучастников и орудия преступления, выявить важные обстоятельства, имеющие значение для уголовного дела.

Автор статьи исследовал научную методику диагностики личностных качеств лица, позволяющих сформировать его психологический портрет, а также спрогнозировать модель поведения в будущем — метод профилирования (профайлинга) лица, изучил аутентификационные системы на основе искусственного интеллекта, позволяющие получить доступ ко всей базе данных конкретного аккаунта, оценить статистику (количество заходов на страницу, активность аккаунта и другое) и сформировать полную базу данных о пользователе, предложил алгоритм реализации получения информации из социальной сети.

**Ключевые слова:** цифровой профиль лица, профайлинг, открытые источники информации, цифровая платформа уголовного судопроизводства, информационные технологии

**Для цитирования:** Моругина Н. А. Социальная сеть как актуальный инструмент при выявлении, раскрытии и расследовании преступлений // Правопорядок: история, теория, практика. 2025. № 4 (47). С. 61–68. DOI: 10.47475/2311-696X-2025-47-4-61-68

Research article

## SOCIAL MEDIA AS AN EFFECTIVE TOOL FOR IDENTIFYING, SOLVING AND INVESTIGATING CRIMES

Nadezhda A. Morugina

*Voronezh Institute of the Ministry of the Interior of Russia, Voronezh, Russia*  
moruginy@mail.ru

**Abstract.** The article substantiates promising directions of using information obtained from a social network (digital footprint) in order to identify, disclose and investigate crimes, and provides the experience of Canada and Russia.

The author argues that the information contained on personal pages of social networks allows to identify the identity of the suspect/accused/witness/victim, to find accomplices and tools of the crime, to identify important circumstances of importance for the criminal case. The author of the article studied a scientific method for diagnosing a person's personality traits, which allows for the creation of a psychological profile and the prediction of future behavior. The method involves profiling (profiling) a person and studying authentication systems based on artificial intelligence, which provide access to the entire database of a specific account, allowing for the evaluation of statistics (such as the number of page visits, account activity, and more) and the creation of a comprehensive user database.

**Keywords:** digital person profile, profiling, open information sources, digital criminal justice platform, and information technologies

**For citation:** Morugina NA. Social media as an effective tool for identifying, solving, and investigating crimes. *Pravoporyadok: istoriya, teoriya, praktika* [Legal and Order: History, Theory, Practice]. 2025;(4):61-68. DOI: 10.47475/2311-696X-2025-47-4-61-68 (In Russ.)

## Введение

Публикации в социальных сетях, сообщения, отправленные посредством электронной почты или мессенджера, покупки в интернет-магазинах, серфинг-сайт, использование поисковых, информационных, развлекательных, учебных и других функций сети «Интернет» — все это формирует так называемые цифровые следы [1, с. 243], представляющие собой комбинацию цифр, которую не так легко уничтожить<sup>1</sup>, но с их помощью возможно восстановить картину произошедших событий.

Каждый человек имеет свой цифровой отпечаток в информационно-коммуникационной сети, а полученная «цифровая информация является содержательным воплощением цифрового следа» [2, с. 101], где цифровой след – это уникальный набор *отслеживаемых цифровых действий*, поступков и коммуникаций, проявляющихся в Интернете или на цифровых устройствах<sup>2</sup>.

В зависимости от активности лица в сети «Интернет» ученые выделяют два вида цифрового следа: активный (информация (данные), которую пользователь размещает в открытых источниках намеренно и осознанно) и пассивный (информация (данные), которую пользователь оставляет в коммуникационной сети невольно) [1, с. 243–246]. Социальная сеть — это онлайн-платформа с открытым публичным профилем, используемая для общения, знакомств, создания социальных отношений между лицами, имеющими схожие интересы или офлайн-связи<sup>3</sup>, облегчающая обмен информацией и агрегирование контента среди виртуальных сообществ или «лицом к лицу».

## Материалы и методы

В ходе проведенного исследования активно использовались общенаучные методы (анализа и синтеза, обобщения, индукции, дедукции и т. д.), а также частнонаучные методы (сравнительно-правовой, технико-юридический).

## Описание исследования

В соответствии с Распоряжением Правительства РФ от 02.09.2022 № 2523-р социальные сети «ВКонтакте» и «Одноклассники» определены как информационные

<sup>1</sup> В сети «Интернет» следы преступления – это комбинация цифр, которые, казалось бы, легко уничтожить, но это не так. Удаленные записи могут сохраняться в кэше поисковых систем, в интернет-архиве и у администраторов сайтов. URL: <https://samara.sledcom.ru/folder/879154/item/1923065/> (дата обращения: 15.05.2026).

<sup>2</sup> Digital footprint. URL: [https://translated.turbopages.org/proxy\\_u/en-ru.ru.ab8e6587-6800b549-2af4b696-74722d776562/https/en.wikipedia.org/wiki/Digital\\_footprint](https://translated.turbopages.org/proxy_u/en-ru.ru.ab8e6587-6800b549-2af4b696-74722d776562/https/en.wikipedia.org/wiki/Digital_footprint) (дата обращения: 15.05.2026).

<sup>3</sup> Социальная сеть. URL: [https://ru.wikipedia.org/wiki/Социальная\\_сеть](https://ru.wikipedia.org/wiki/Социальная_сеть) (дата обращения: 15.05.2026).

системы и (или) программы для электронных вычислительных машин, используемые государственными органами и судами для создания официальных страниц<sup>4</sup>. Между тем существует отличие социальных сетей от страниц интернет-сайтов, заключающееся в формировании контента, т. е. информационного наполнения аккаунта, который создает само лицо (пользователь сети), делая свои персональные данные общедоступными. Вся информация, размещенная в социальной сети открытого профиля и контента страницы<sup>5</sup>, является публичной, кроме случаев установления конфиденциальности аккаунта.

Согласно данным We Are Social и Meltwater Digital, число активных пользователей социальных сетей в 2024 г. превысило 5 миллиардов (5,04 миллиарда), что эквивалентно 62,3 % населения Земли и составило 5,6 % ежегодного прироста<sup>6</sup>. При этом средний пользователь социальных сетей в 2024 году проводит в сети 2 часа 23 минуты в день.

Отметим, что в США социальные сети и персональные страницы (профиль) активно используют при расследовании преступлений как ценный инструмент для поиска и сбора информации [3, с. 30–31]. Еще в 1976 году генерал-лейтенант армии Samuel V. Wilson, руководивший Разведывательным управлением Министерства обороны США, отмечал, что при расследовании преступлений «90 % разведанных приходит из открытых источников и только 10 за счёт работы агентуры»<sup>7</sup>.

Напомним, что технология социальных сетей включает в себя множество компонентов: контент, подписку, чат, персонализацию, бэкенд (серверную часть системы), базу данных, API, фронтенд (пользовательский интерфейс), аутентификацию и авторизацию, масштабируемость и т. д., обеспечивающих функциони-

<sup>4</sup> Распоряжение Правительства РФ от 02.09.2022 № 2523-р «Об определении «ВКонтакте» и «Одноклассники» в качестве информационных систем и (или) программ для электронных вычислительных машин, используемых государственными органами, в том числе судами, Судебным департаментом при Верховном Суде Российской Федерации, включая управления Судебного департамента при Верховном Суде Российской Федерации в субъектах Российской Федерации, а также органами местного самоуправления, организациями, подведомственными государственным органам и органам местного самоуправления, для создания официальных страниц» // Собрание законодательства РФ. 2022. № 37. Ст. 6381.

<sup>5</sup> Электронная информация, которой наполняется аккаунт.

<sup>6</sup> We Are Social + Meltwater Digital 2024 report: Global social media users pass 5bn milestone (Отчёт We Are Social + Meltwater Digital за 2024 год число пользователей социальных сетей в мире превысило 5 млрд). URL: <https://campaignbrief.com/we-are-social-meltwater-digital-2024-report-global-social-media-users-pass-5bn-milestone/> (дата обращения: 15.05.2026).

<sup>7</sup> Разведка по открытым источникам. URL: <https://ru.wikipedia.org/wiki/> (дата обращения: 16.05.2026).

рование и взаимодействие пользователей в онлайн-пространстве.

*Личная страница пользователя* в социальной сети, где он указывает информацию о себе, называется *аккаунт* или *профиль*.

Аккаунт — это идентификатор пользователя (login) и его пароль, который чаще всего хранится в зашифрованном или хэшированном виде с целью обеспечения безопасности [4, с. 295]. Профиль лица также представляет собой учётную запись пользователя, вход к которому осуществляется с помощью логина, номера телефона, e-mail и пароля.

Таким образом, **социальная сеть — это общая среда, а профиль (или аккаунт) в социальной сети — конкретная страница пользователя**, где он представляет свою *цифровую личность* как «образ, им созданный в виртуальном пространстве в виде активного и пассивного цифрового следа» [5, с. 48] (контур деятельности субъекта в цифровой среде). Соглашаясь с утверждением ученых о том, что виртуальный образ цифрового профиля лица «может быть как адекватным отражением истинных характеристик его личности, так и тщательно выстроенной иллюзией» [5, с. 49], считаем, что для формирования целостного представления о возможности вычленения правоохранительными органами из аккаунта социальной сети электронной информации, необходимой для раскрытия и расследования преступления, определенный научный интерес представляет изучение самого феномена «цифровой профиль лица в социальной сети».

*Цифровой профиль лица в социальной сети* — это совокупность электронной информации о человеке, хранящейся в онлайн-пространстве.

А. А. Лебедев, В. А. Парфенов цифровой профиль в социальной сети рассматривают как данные, привязанные к конкретному лицу и подтверждающие его право пользоваться и распоряжаться аккаунтом [6, с. 96]. Т. Г. Какохо трактует цифровой профиль лица как совокупность цифровых данных (записей), содержащихся в той или иной информационной системе, размещенной в цифровом пространстве [7, с. 81].

Интересной представляется модель цифрового профиля лица как элемента информационно-технической стратегии расследования преступлений, описанная О. А. Зайцевым и П. С. Пастуховым, состоящая из четырех групп индикаторов<sup>1</sup>:

- 1) анкетные персональные данные;
- 2) регистрационные данные субъектов и объектов в цифровой системе правоотношений;

<sup>1</sup> Идентификатор — это уникальное обозначение сведений о лице, применяется для его идентификации в соответствии с нормативными правовыми актами путем применения технических и (или) технологических способов. См.: Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (с изменениями и дополнениями). URL: <https://base.garant.ru/12148555/> (дата обращения: 15.05.2026).

3) биометрические персональные данные в цифровой инфраструктуре;

4) цифровые идентификаторы оконечного оборудования, информационных систем и компьютерных сетей [4, с. 281].

В этой связи Е. А. Гамбарова справедливо отмечает, что социальные сети являются новым источником информации, которую следователь может использовать в своей работе [3, с. 30–31].

Обозначим, что с января по декабрь 2024 года было зарегистрировано 765,4 тыс. преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, что на 13,1 % больше, чем за аналогичный период прошлого года. При этом 84,8 % преступлений совершаются с использованием социальных сетей (649,1 тыс.; +23,2 %) и почти половина (45,2 %) — средств мобильной связи (346 тыс.; +14,3 %)<sup>2</sup>.

В этой связи положительно оцениваем позицию С. В. Зуева, который предлагает увеличить отделы «К», специализирующиеся на расследовании преступлений с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, за счет повышения квалификации действующих сотрудников, а также принятия в штат специалистов-программистов [8, с. 87].

*Приведем несколько примеров раскрытия преступлений с использованием социальных сетей (опыт Канады и России):*

1. 25 марта 2015 года около 6 часов в канадской провинции Саскачеван на проселочной дороге неподалеку от свалки проезжавший мимо водитель нашел тело неизвестной девушки.

Сотрудники полиции на месте происшествия обнаружили ремень (с которого было выделено две ДНК), а осмотрев тело — странгуляционную борозду, характерную для удушения.

После возбуждения уголовного дела по признакам преступления, предусмотренного St. 222 of the Criminal Code of Canada (ст. 222 Уголовного кодекса Канады) — «Умышленное убийство», в целях идентификации личности неизвестной в социальной сети открытого доступа сотрудники полиции разместили фотографию ее татуировок.

А. Стори (подруга убитой), узнав татуировки, опознала потерпевшую, рассказав о том, что 24 марта 2025 года Б. Гаргол (убитая) проводила время с А. Шайенн (лучшая подруга убитой). Изучив социальные сети обеих, сотрудники полиции обнаружили их совместное «селфи», сделанное в день убийства, на котором было орудие убийства — ремень. А. Штейн призналась в преступлении и была приговорена к семи годам лишения свободы<sup>3</sup>.

<sup>2</sup> Краткая характеристика состояния преступности в Российской Федерации за январь-декабрь 2024 года. URL: [https://portal.tpu.ru/SHARED/n/NIKOLAENKOV/student/risk\\_](https://portal.tpu.ru/SHARED/n/NIKOLAENKOV/student/risk_) (дата обращения: 16.05.2026).

<sup>3</sup> На этом фото есть орудие убийства: селфи в соцсетях помогло

2. В 2015 году в г. Перми неизвестный мужчина напал на 20-летнюю девушку, изнасиловал и похитил принадлежащие ей ценные вещи, после чего скрылся с места происшествия.

Пострадавшая написала заявление в полицию, где был составлен фоторобот преступника.

Однако преступление было раскрыто, благодаря социальной сети «ВКонтакте», где, зайдя в свой профиль, потерпевшая обнаружила эмодзи «мне нравится», под одной из своих фотографий. Нажав на счётчик просмотров, и перейдя на страницу лица, отметившего ее фото, потерпевшая опознала преступника.

Фотография профиля «ВКонтакте» совпала с фотороботом подозреваемого. Установив IP-адрес лица, сотрудники правоохранительных органов определили его местоположение, после чего задержали.

3. В ноябре 2020 года в полицию г. Чебоксар обратилась с заявлением о преступлении местная жительница, которая требовала привлечь к уголовной ответственности неизвестное лицо, ведущее непристойную переписку в социальной сети с её 9-летней дочерью.

Ввиду того что преступление было совершено в отношении несовершеннолетней, материалы проверки были переданы в СУ СК РФ по Чувашской Республике.

Было установлено, что подозреваемый вел переписку с одного аккаунта «Пашка Данилов» по несколько раз в день с разными пользователями (31 потерпевшая в возрасте от 9 до 15 лет) на протяжении полутора лет. В ходе расследования преступления следователем было изучено 3382 диалога с пользователями соцсети и запрошены сведения обо всех IP-адресах, которые выделялись при выходе в социальную сеть на страницу подозреваемого, и установлен IMEI и модель устройства, которым он пользовался.

Для подтверждения связи преступника со всеми потерпевшими необходимо было установить номер его телефона. Однако при получении телефонной детализации выяснилось, что в каждой переписке фигурировали разные номера. Сравнив выгрузку по IP-адресам, детализацию телефонных соединений и проанализировав более терабайта информации, было выявлено несколько технических устройств, с которых велась электронная переписка.

С целью установления личности подозреваемого была запрошена и изучена детализация всех телефонных соединений абонентских номеров. Выяснилось, что почти все номера были зарегистрированы в других регионах (позднее было установлено, что номера зарегистрированы на бывших сослуживцев и вахтовиков), и только один — в Чувашии. Им владела женщина, которая была допрошена. В ходе допроса свидетель пояснила, что познакомилась с гр. Н. в социальных сетях, описала его внешность, автомобиль и сообщила номер телефона, по которому и был установлен подозреваемый.

Изъяв технические устройства и телефон подозреваемого, проведя криминалистическую экспертизу, раскрыть преступление. URL: <https://tech.onliner.by/2024/08/12/facebook-selfie> (дата обращения: 15.05.2026).

было установлено, что IMEI телефона гр. Н. идентичен IMEI устройства преступника.

Суд признал гр. Данилова виновным в совершении 11 эпизодов преступлений, предусмотренных п. «б» ч. 4 ст. 132 УК РФ (насильственные действия сексуального характера, совершённые с использованием беспомощного состояния потерпевших, не достигших 14-летнего возраста), ч. 3 ст. 135 УК РФ (развратные действия) и 6 эпизодов, предусмотренных п. «б» ч. 3 ст. 242 УК РФ (незаконный оборот порнографических материалов среди несовершеннолетних). Приговорён к 11 годам лишения свободы с отбыванием наказания в колонии строгого режима<sup>1</sup>.

Метод изучения личности преступника в сети «Интернет» возник в конце 70-х годов XX века, когда профессор Национальной академии ФБР США Д. Дуглас основал отдел бихевиористики психологического анализа поведения преступника, возглавив национальную программу исследований «Личностно-преступное профилирование преступника». Одним из тактических приемов метода профилирования считалась технология поиска, сбора и анализа информации в открытых источниках, названная OSINT (от англ. Open Source Intelligence).

*Профилирование (профайлинг) лица* на основе анализа аккаунта в социальных сетях представляет собой интегрированный метод поведенческого анализа личности, позволяющий сформировать психологический портрет лица, а также спрогнозировать модель его типичного поведения, исследовав его цифровой профиль по следующим направлениям:

- внешность лица (стиль одежды, наличие аксессуаров, типичные позы, открытость взгляда и т. д.);
- фотоизображения пользователя (сюжеты, содержание, цветовая гамма, частота обновления);
- статусы (обновляемость, содержание);
- онлайн-сообщества (сфера интересов);
- посты, цитаты, репосты и перепосты (анализируется их структура, стилистика, периодичность, тематика, содержание);
- анкетные данные и профессиональные достижения;
- окружение (устанавливается круг знакомств и контактов).

Из этого следует, что личная страница пользователя в социальной сети является его «цифровым профилем», отражающим персональные данные, внутреннее состояние лица, склонность к определенным действиям. Детальный анализ цифрового профиля способствует составлению предварительного «цифрового портрета», содержащего следующую электронную информацию:

- регистрационные данные (имя, фамилия, пол, возраст, место жительства, номер телефона, e-mail и другие сведения, которые пользователь размещает в свободном доступе при создании аккаунта);

<sup>1</sup> URL: Киберпреступление и реальное наказание. [https://dzen.ru/a/YuI8NAX\\_a3NZ-Xir](https://dzen.ru/a/YuI8NAX_a3NZ-Xir) (дата обращения: 16.05.2026).

– информация о пользователе (отражает всю текущую информацию на странице: профессия, семейное положение, интересы, все изменения в профиле: номера телефона и его привязки, смена работы, города, семейного статуса);

– действия пользователя в сети (фотографии, которые выкладываются, посты, лайки<sup>1</sup>, хештеги<sup>2</sup>, репосты<sup>3</sup>, комментарии, просмотренные видео, просмотр других профилей, контент, который читается или удаляется из ленты, сообщения);

– подписки на сообщества и история подписок, а также публикации в них;

– список друзей, история их добавления на свою страницу;

– исходящие и входящие контакты, в том числе из других соцсетей.

– данные об устройстве входа (операционная система, модель телефона, браузер, IP-адрес, установленные приложения, уровень заряда батареи);

– геоданные (местоположение пользователя и его перемещения с методанными);

– cookie-файлы (текстовые файлы с информацией, которые сайты хранят на устройстве пользователя. К примеру, данные логина, e-mail и пароль, которые заполняются автоматически при повторном входе и т. д.

*Сетевой профайлинг* возник с совершенствованием информационно-коммуникационных технологий, а с появлением социальных сетей получил свое распространение. В частности, в 2004 году при учреждении социальной сети Facebook<sup>4</sup> исследовательские подразделения компании-владельца получили доступ к цифровому профилю лица, оставленного им в информационном пространстве<sup>5</sup>.

Изначально с целью предупреждения преступлений, в том числе с помощью социальных сетей, некоторые страны вносили изменения в действующее законодательство. Так, к примеру, в 2007 году во Франции был принят Закон № 2007-297 «О предупреждении преступности», предусматривающий использование сотрудниками органов внутренних дел «фейковых» учетных записей («псевдонимов» — Enquetes sous pseudonyme) в социальных и иных сетях для проведения расследований в Интернете.

<sup>1</sup> Форма одобрения контента в социальных сетях (способ выразить свое одобрение, положительное отношение к чему-либо). Алгоритмы социальных сетей учитывают лайки, определяя, какой контент необходимо продвигать. URL: <https://www.unisender.com/ru/glossary/chto-takoe-lajk/?ysclid=m9qt8ryf9926475607> (дата обращения: 17.05.2026).

<sup>2</sup> Метка в виде решётки и ключевого слова или слов после неё, написанных без пробелов, используемая для систематизации контента в социальных сетях.

<sup>3</sup> Репост в социальной сети – это действие, при котором пользователь делится чужим контентом со своими подписчиками.

<sup>4</sup> Является продуктом корпорации Meta, запрещенной на территории Российской Федерации.

<sup>5</sup> NYT: Facebook предоставляла десяткам компаний доступ к личным данным пользователей. URL: <https://tass.ru/obschestvo/5929612> (дата обращения: 15.05.2026).

В мае 2025 года Минцифры России опубликовали проект постановления Правительства «Об установлении правил предоставления владельца агрегатора сведений с использованием системы межведомственного электронного взаимодействия по запросу уполномоченного государственного органа, осуществляющего оперативно-розыскную деятельность или обеспечение безопасности Российской Федерации» с перечнем обязательной для предоставления информации.

Из документа следует, что правоохранительные органы в целях раскрытия и расследования преступлений смогут запрашивать, следующую информацию:

– регистрационные данные пользователя агрегатора (номер телефона, адрес электронной почты и др.);

– дату и время доступа пользователя к агрегатору, а также IP-адрес;

– информацию о товарах, работах и услугах, которые пользователь разместил на агрегаторе;

– сведения о товарах и услугах, которые пользователь заказывал на агрегаторе (название товара или услуги, их цена, адрес доставки, способ оплаты, комментарии к заказу).

А также установлен срок исполнения запроса правоохранительных органов — не менее 24 часов<sup>6</sup>.

Кроме того, в целях раскрытия и расследования преступлений в цифровом пространстве и мониторинга электронной информации о лице в социальной сети были созданы специальные системы поиска.

В 2008 году студенты-психологи Кембриджского университета Дэвид Стиллзуэлл и Михал Косински создали одно из первых приложений, собирающих и анализирующих информацию о пользователях социальных сетей — myPersonality — «Моя личность»<sup>7</sup>.

С 2011 года самое популярное в Китае приложение для обмена электронными данными WeChat, сочетающее в себе социальную сеть, платёжную систему, платформу для шоппинга и игр и многое другое, находится под постоянным мониторингом полиции. Любое сообщение, отправленное через социальную сеть, отслеживается китайским технологическим гигантом Tencent, оператором приложения. Все сообщения хранятся в браузере в течение шести месяцев, удалённые могут быть восстановлены по запросу правоохранительных органов к оператору.

Кроме того, правительство Китая потребовало от пользователей Sina Weibo (сайт микроблогов в социальной сети), чтобы все зарегистрировались под своими настоящими идентификационными именами. При отказе от такой регистрации пользователи не могли

<sup>6</sup> Обозначенные Правила вступают в силу с 1 сентября 2025 года. URL: <https://regulation.gov.ru/Regulation/Npa/PublicView?npaID=156913&ysclid=maxmx8whig215345372> (дата обращения: 15.05.2026).

<sup>7</sup> Scholars Have Data on Millions of Facebook Users. URL: [https://translated.turbopages.org/proxy\\_u/en-ru.ru.4f46fb87-68243c3f-38091481-74722d776562/https/www.nytimes.com/2018/05/06/technology/facebook-information-data-sets-academics.html](https://translated.turbopages.org/proxy_u/en-ru.ru.4f46fb87-68243c3f-38091481-74722d776562/https/www.nytimes.com/2018/05/06/technology/facebook-information-data-sets-academics.html) (дата обращения: 25.05.2026).

публиковать, «постить» или комментировать посты на сайте<sup>1</sup>.

В 2015 году по заказу Королевской Канадской Конной Полиции (Royal Canadian Mounted Police, RCMP) был создан поисковый робот *habr.com*, изучающий DeepWeb (глубины интернета) на предмет торговли незаконными товарами и предложений услуг.

В 2017 году полиция Дании разработала собственную систему поиска ЕСЗ, способную сопоставлять активность в DeepWeb с криптовалютной активностью пользователя, для выявления преступных схем<sup>2</sup>.

С 2020 года в Китайской Народной Республике активно применяют системы «Полицейского облака» для сбора данных об активности в социальных сетях и просмотре интернет-страниц, а также отслеживания и прогнозирования деятельности активистов, диссидентов и этнических меньшинств<sup>3</sup>.

Отметим, что в настоящее время существует несколько *методов сбора электронной информации о лице в социальной сети*.

Выделим самые распространённые из них:

1. Web-scraping («веб-скреппинг») — автоматизированный метод извлечения данных с сайтов, позволяющий собирать информацию в сети при помощи специально созданной программы или бота-скрапера, имитирующего действия пользователя и позволяющего получить доступ к содержимому веб-страниц.

2. Web crawler («веб-паук») — метод сбора данных для дальнейшей обработки, используемый во всех поисковых системах. Программа в автоматическом режиме осуществляет поиск страницы объекта, ее сканирование (текстовое содержание веб-страницы, теги и гиперссылки) и передачу (загрузку) собранных данных на специальный сервер.

На сегодняшний момент для мониторинга социальных сетей правоохранительные органы России используют специальные программные комплексы на основе искусственного интеллекта, среди которых:

1. «Демон Лапласа» (LD 3.0) — автоматизированная система круглосуточного мониторинга и сбора данных из сети «Интернет», позволяющая извлекать, собирать и анализировать электронную информацию цифрового профиля лица из социальных сетей, таких как: «ВКонтакте», «Одноклассники»<sup>4</sup>.

Ключевые аспектами работы АИС «Демон Лапласа» (LD 3.0) являются: автоматический поиск запрещённого контента, к примеру мониторинг материалов,

содержащих публичные призывы к экстремистской деятельности или оправдывающих её, отслеживание информационно-пропагандистской политики радикальных исламских организаций, информирование о возможных готовящихся акциях протеста и т. д.

2. «Виток-OSINT»<sup>5</sup> — информационно-поисковая система, позволяющая сотрудникам правоохранительных органов получать информацию из открытых источников, анализировать её, фильтровать и сортировать результаты. Система «Виток-OSINT» обладает развитыми средствами контроля получения данных из внешних источников, а также визуализации обработанных данных, позволяет существенно сократить время поиска информации, тем самым освобождая сотрудника полиции от длительной рутинной работы. Скорость выполнения поисковых запросов при помощи АПК «Виток-OSINT» в среднем на 300 % быстрее, а полнота выявленной информации на 20 % больше, чем при выполнении запросов в ручном поиске.

3. Search4face — веб-сервис, помогающий осуществлять поиск лица по фотографии, преимущественно из профилей в социальных сетях: «ВКонтакте», «Одноклассники»<sup>6</sup>.

4. «Крибрум. Публичный поиск» — информационно-поисковая система для постоянного оперативного мониторинга аккаунта в социальной сети (Facebook<sup>7</sup>, «ВКонтакте», Twitter<sup>7</sup>, Instagram<sup>7</sup>, «Одноклассники», «Ответы Mail.ru») <sup>8</sup>.

Программный комплекс «Крибрум. Публичный поиск» обеспечивает постоянный мониторинг русскоязычных текстовых публикаций, представленных в форме пользовательского и редакционного контента, в том числе в виде новостей, статей, комментариев, постов, твитов, записей и т. п., в открытых интернет-источниках, относящихся ко всем типам социальных медиа, включая, но не ограничиваясь социальными сетями (не менее 220 миллионов аккаунтов). Система собирает и обрабатывает около 95 млн информационных сообщений из социальных медиа в сутки. Мониторинг осуществляется с помощью поисковых роботов — спайдеров<sup>9</sup>.

5. «Сеус» — поисковая система, разработанная в 2024 году пермской компанией «Сеуслаб»<sup>10</sup>, позволя-

<sup>5</sup> 7 апреля 2020 года на основании приказа Минкомсвязи России от 07.04.2020 № 162 «О включении сведений о программном обеспечении в единый реестр российских программ для электронных вычислительных машин» комплекс Виток-OSINT добавлен в единый реестр российских программ. URL: <https://reestr.digital.gov.ru/reestr/307657/> (дата обращения: 18.05.2026).

<sup>6</sup> Search4face. URL: <https://search4faces.com/?ysclid=ma6e8lots148764847> [https://www.securitylab.ru/analytics/557590.php?lang=ru&utm\\_referrer=https%3A%2F%2Fya.ru%2F](https://www.securitylab.ru/analytics/557590.php?lang=ru&utm_referrer=https%3A%2F%2Fya.ru%2F) (дата обращения: 18.05.2026).

<sup>7</sup> Является продуктом корпорации Meta, запрещенной на территории Российской Федерации.

<sup>8</sup> Крибрум. Публичный поиск. URL: <https://kribrum.ru/upload/pubsearch.pdf> (дата обращения: 25.05.2026).

<sup>9</sup> Спайдер — программа, выполняющая задачу просмотра и сбора необходимой информации, работающая по своей области интернета (социальные сети, сайты, форумы, блоги и т. д.).

<sup>10</sup> Математическую модель к поисковой программе «Сеус» на-

<sup>1</sup> No Alias for Weibo Users in China. URL: <https://www.yahoo.com/news/no-alias-weibo-users-china-143022142.html> (дата обращения: 25.05.2026).

<sup>2</sup> Как ловят преступников в Deep Web. URL: [https://vk.com/wal1-112486442\\_2448?ysclid=mancrejlgz61067280](https://vk.com/wal1-112486442_2448?ysclid=mancrejlgz61067280) (дата обращения: 25.05.2026).

<sup>3</sup> Mass surveillance in China URL: [https://translated.turbopages.org/proxy\\_u/en-ru.ru.75cb7fa3-682407a9-44ab6fa8-74722d776562/](https://translated.turbopages.org/proxy_u/en-ru.ru.75cb7fa3-682407a9-44ab6fa8-74722d776562/) [https://en.wikipedia.org/wiki/Mass\\_surveillance\\_in\\_China](https://en.wikipedia.org/wiki/Mass_surveillance_in_China) (дата обращения: 25.05.2026).

<sup>4</sup> Демон Лапласа. URL: <https://protestonline.ru/?ysclid=m9sg01pvvr901654569> (дата обращения: 25.05.2026).

ющая выявлять потенциально опасных пользователей социальных сетей, в том числе распространяющих экстремистскую идеологию, анализируя открытые профили, группы, лайки и комментарии, а также поведение пользователей в сети.

### Заключение и вывод

В целях эффективного раскрытия и расследования преступлений с учетом имеющихся технологических программных комплексов, способных выявлять потенциально опасных пользователей социальных сетей на основе полученной электронной информации о лице, рекомендуем:

1. Создать *Единую поисковую информационную систему открытого мониторинга* с возможностью анализа неограниченного количества аккаунтов и групп социальных сетей, интегрировав ее в защищенный контур *Единой системы информационно-аналитического обеспечения деятельности МВД России (ИСОД МВД России)*.

2. *Получение информации из открытых источников*, таких как социальная сеть, сбор которой необходимо осуществлять в соответствии с УПК РФ посредством **истребования**, определяемого нами как *иное процессуальное действие*, должен включать в себя следующий алгоритм его реализации:

– определить цель и объем сбора информации: установить, какие сведения обязательны для расследования преступления (исследовать профиль лица,

писали научные сотрудники Пермского государственного национального исследовательского университета (ПГНИУ). URL: <https://iz.ru/1784029/maria-frolova/onlain-dozor-v-rossii-sozdali-sistemu-dla-vyavlenia-ekstremistov-v-socsetah> (дата обращения: 16.05.2026).

лайки, репосты, публикации, либо провести мониторинг аккаунтов; определить конкретный почтовый ящик и временной диапазон для сбора данных, либо конкретное устройство или платформу и т. д.);

– осуществить сбор информации свободного доступа: произвести сохранение (техническую фиксацию<sup>1</sup>) общедоступных данных (посты, комментарии, фото и видеофайлы, списки «друзей», публичные сообщения) с датой и временем получения данных (скриншот, экспорт данных);

– оформить и направить официальный запрос (в администрацию социальной сети, провайдеру электронной почты или владельцу устройства) для получения закрытой или удаленной информации (переписка, IP-адреса, лог-файлы и т. д.), при необходимости получить законное право на доступ к информации: согласие владельца либо суда для производства сбора содержимого аккаунта, почтового ящика или конкретного устройства;

– произвести техническую фиксацию и сохранение электронной информации с применением автоматизированного метода извлечения и специальных технических устройств, предназначенных для сбора и хранения информации без искажения, которая должна происходить следующим образом: осуществить экспорт данных, создать копию необходимой информации в неизменном виде (скриншот, запись экрана) с указанием метаданных: дата, время, URL и т. д., произвести архивирование файлов с сохранением структуры и метаданных, используя, к примеру, хеш-код.

<sup>1</sup> Техническая фиксация информации представляет собой комплекс мероприятий, направленных на сохранение, документирование и подтверждение подлинности цифровых данных.

### Список источников

1. Худяков В. В., Ананьев А. А. Цифровые следы // Криминологический журнал. 2023. № 4. С. 243–246.
2. Русман Г. С., Родионов В. С. Цифровая информация как содержательный элемент компонентов цифровой индустрии с позиции права (на примере кибербезопасности) // Гражданское и уголовное судопроизводство. 2020. № 5(79). С. 100–104.
3. Гамбарова Е. А. К вопросу об использовании информации из социальных сетей в работе следователя // Вектор науки ТГУ. Серия: Юридические науки. 2017. № 1(28). С. 30–31.
4. Зайцев О. А., Пастухов П. С. Цифровой профиль лица как элемент информационно-технологической стратегии расследования преступлений // Вестник Пермского университета. Юридические науки. 2022. Вып. 56. С. 281–308.
5. Тархов С. В., Тархова Л. М., Назарова Ю. Р. Цифровые двойники человека и личности в организационных системах // Современные наукоемкие технологии. 2025. № 3. С. 47–52.
6. Лебедев А. А., Парфенов В. А. Наследование цифровых профилей на виртуальных платформах // Актуальные проблемы отраслевой юридической науки: доклады участников XIV Международной научно-практической конференции и V Международной научно-практической конференции, Владимир. 2025. С. 95–98.
7. Какохо Т. Г. Правовые основы единого цифрового профиля гражданина // Наука. Общество. Государство. 2023. Т. 11, № 3. С. 80–90.
8. Зуев С. В. Итоги проведения профессионального круглого стола «Выявление, документирование и расследование преступлений, совершаемых с использованием СМИ, электронных и информационно-коммуникационных сетей // Правопорядок: история, теория, практика. 2018. № 1(16). С. 86–88.

**СВЕДЕНИЯ ОБ АВТОРЕ**

**Моругина Надежда Анатольевна**

Кандидат юридических наук, доцент, доцент кафедры уголовного процесса, Воронежский институт МВД России  
Россия, 394065, Воронеж, проспект Патриотов, 53  
E-mail: moruginy@mail.ru

**INFORMATION ABOUT THE AUTHOR**

**Nadezhda A. Morugina**

Candidate of Legal Science, Associate Professor of the chair of Criminal Procedure, Voronezh Institute of the Ministry of the Interior of Russia  
53 prospect Patriotov, Voronezh 394065, Russia.  
E-mail: moruginy@mail.ru

**КОНФЛИКТ ИНТЕРЕСОВ**

Конфликт интересов отсутствует.

**CONFLICT OF INTEREST**

There is no conflict of interest.

Дата поступления статьи / Received: 07.07.2025.

Дата рецензирования статьи / Revised: 19.08.2025.

Дата принятия статьи к публикации / Accepted: 15.10.2025.